SSRF Cheat Sheet

Definition of the SSRF vulnerability

Web vulnerability that enables to interact with a server (internal or external network, or the host itself)
Can give access to files, services (for example web, FTP, SMTP, SQL/NoSQL, etc.) on the vulnerable server or on another server of the internal network of the server, to other servers or networks, to an interface router…

Where to find it?

As soon as a functionality interacts with an external resource.
For example:

- Uploading a file
- API calls
- Webhooks
- Redirecting to a page
- Document parsers
- Documents generators (pdf…)

Types

- Content-based
- Boolean-based
- Error-based
- Time-based

Exploitation

√ Bypassing filters

- **0.0.0.0 variants**
  - › 0
  - › [::]
  - › 0000
  - › 017700000001
  - › 0x7f000001
- **localhost & variants**
  - › localhost
  - › 127.0.0.1
  - › A domain with a redirection to 127.0.0.1
    - o you own
    - o spoofed.burpcollaborator.net
    - o 127.0.0.1.nip.io
  - › Short IP
    - o 127.0.1
    - o 127.1
  - › Change of base
    - o 2130706433 (decimal IP)
    - o 017700000001 (octal IP)
    - o 0x7f001 (hexadecimal IP)
  - › IP V6
    - o [::1]
    - o [::ffff:127.0.0.1]
    - o [::127.0.0.1]

√ Common URL scheme

- file://
- http://
- ftp://
- gopher://
- dict://
- idapt://

√ Bypassing DNS filters (DNS rebinding method)

- Rbndr

Example to switch between 192.168.0.1 and 127.0.0.1:
7f000001.c0a80001.rbndr.us

Protection

White listing needed resources
- Defining authorised DNS names / IP addresses
- Defining authorised protocols

vaadata
Ethical Hacking Services
www.vaadata.com
v2022.1